

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-234261

(43)Date of publication of application : 27.08.1999

(51)Int.Cl.

H04L 9/10

H01L 27/04

H01L 21/822

H04L 9/14

(21)Application number : 10-048853

(71)Applicant : NIPPON TELEGR & TELEPH
CORP <NTT>

(22)Date of filing : 13.02.1998

(72)Inventor : FUJII KOJI

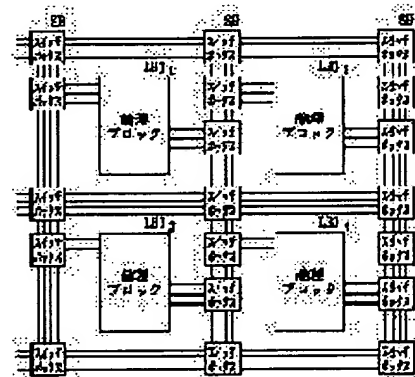
(54) INTEGRATED CIRCUIT

(57)Abstract:

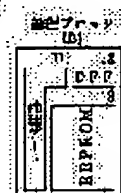
PROBLEM TO BE SOLVED: To attain dispersion of elements to be analyzed by storing program data for realizing an enciphering function and enciphered key data in a memory inside a programmable logical gate.

SOLUTION: Program data (d) for characterizing an enciphering circuit and enciphering key data (k) are stored on a non-volatile memory (EEPROM) 13 arranged in a programmable logical gate in an integrated circuit 101. That is, an enciphering function is composed of a programmable logical gate that takes a logical block LB 1 as an element, and a parameter for characterizing the enciphering function is made to be the enciphering key data (k) and the program data (d) and increases more than a conventional parameter. Moreover, each parameter of the enciphering key data (k) and the program data (d) is physically stored on one EEPROM 13 on hardware, both parameters of the enciphering key data (k) and the program data D are made difficult for the third party to discriminate.

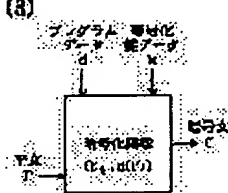
(1) 応答回路



(2)



(3)



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-234261^V

(43) 公開日 平成11年(1999) 8月27日

(51) Int.Cl.⁶

識別記号

F I

H 0 4 L 9/10

H 0 4 L 9/00

6 2 1 A

H 0 1 L 27/04

H 0 1 L 27/04

F

21/822

H 0 4 L 9/00

6 4 1

H 0 4 L 9/14

審査請求 未請求 請求項の数 5 F D (全 7 頁)

(21) 出願番号

特願平10-48853

(22) 出願日

平成10年(1998) 2月13日

(71) 出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72) 発明者 藤井 孝治

東京都新宿区西新宿三丁目19番2号 日本

電信電話株式会社内

(74) 代理人 弁理士 川久保 新一

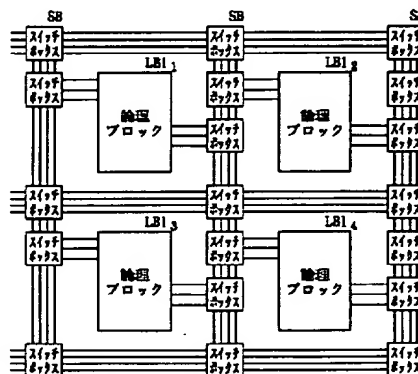
(54) 【発明の名称】 集積回路

(57) 【要約】

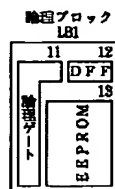
【課題】 動作解析の起点を暗号化鍵データに集中させずに、解析される要素を分散させることができる集積回路を提供することを目的とするものである。

【解決手段】 プログラマブル論理ゲートを用いて、暗号化回路、復号化回路を構成するものであり、プログラマブル論理ゲートのプログラム用記憶回路に、暗号化回路、復号化回路を実現するプログラムデータと、暗号化鍵データとの両者を格納するものである。

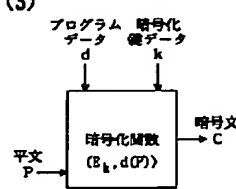
(1) 101: 集積回路



(2)



(3)



【特許請求の範囲】

【請求項 1】 暗号化関数を実現するプログラムデータと暗号化鍵データとが、1つのプログラマブル論理ゲート内のメモリに格納されていることを特徴とする集積回路。

【請求項 2】 復号化関数を実現するプログラムデータと復号化鍵データとが、1つのプログラマブル論理ゲート内のメモリに格納されていることを特徴とする集積回路。

【請求項 3】 暗号化関数を実現するプログラムデータと暗号化鍵データと復号化関数を実現するプログラムデータと復号化鍵データとが、1つのプログラマブル論理ゲート内のメモリに格納されていることを特徴とする集積回路。

【請求項 4】 請求項 1～請求項 3 のいずれか 1 項において、

上記プログラマブル論理ゲートの機能を同一に維持したまま、上記プログラムデータを変更するプログラムデータ変更手段と；上記プログラムデータ変更手段を、上記プログラマブル論理ゲート自身が繰り返して起動する変更起動手段と；を有することを特徴とする集積回路。

【請求項 5】 請求項 1～請求項 3 のいずれか 1 項において、

上記プログラマブル論理ゲートの機能を同一に維持したまま、上記プログラムデータを変更するとともに、上記プログラマブル論理ゲートの外部の信号に応じて、上記プログラムデータの変更動作を起動するプログラムデータ変更手段を有することを特徴とする集積回路。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、秘密情報を扱う集積回路において、不正者による動作解読を防止する集積回路に関するものである。

【0002】

【従来の技術】市販 IC では、多くのユーザの利益に供するために、その内部動作を公開する必要がある。一方、身分証明、電子マネー等に使用される IC では、秘密情報の漏洩を防止するために、その内部動作を隠匿する必要がある。

【0003】図 5 は、従来の集積回路 100 の説明図である。

【0004】秘密情報を取り扱う従来の集積回路では、図 5 (1) に示すように、通常の汎用プロセッサにおける処理方式と同様の方式を採用している場合が多く、セキュリティの保持を、暗号化鍵データと復号化鍵データとの守秘性に頼っている。

【0005】この場合、市販されているデバッグ用ツールを用いれば、様々な命令をプロセッサに実行させることが可能であり、このようにすることによって、暗号化鍵データ、復号化鍵データを読み出すこともできる。

【0006】

【発明が解決しようとする課題】従来例における汎用プロセッサでは、ハードウェアが個別にモジュール化されているので、各モジュールの入出力端子から信号を取り出し、この取り出した信号を解析することによって、暗号化鍵データを傍受することが可能であり、暗号データの生成の仕組みを傍受することが可能である。観念的には、暗号化関数は、暗号化鍵データ k によって一意に決まり、平文を P 、暗号文を C とすると、

$$C = E_k(P)$$

である。しかし、実装形態としては、図 5 (2) に示すように、むしろ暗号化鍵データ k を陽に含む関数

$$C = E(k, P)$$

である。したがって、従来例においては、入力である暗号化鍵データ k 、平文 P と、出力である暗号文 C との対応を傍受できれば、暗号解読の大きなヒントになる。

【0007】上記のように、従来の集積回路 100 においては、汎用プロセッサの動作に関して多少の知識を有していれば、電子マネー等に利用される集積回路の内部動作を解析することができる。したがって、上記従来例においては、入金データ等を不正に変更することが容易であるという問題がある。

【0008】本発明は、動作解析の起点を暗号化鍵データに集中させずに、解析される要素を分散させることができる集積回路を提供することを目的とするものである。

【0009】

【課題を解決するための手段】本発明は、プログラマブル論理ゲートを用いて、暗号化回路、復号化回路を構成するものであり、プログラマブル論理ゲートのプログラム用記憶回路に、暗号化回路、復号化回路を実現するプログラムデータと、暗号化鍵データとの両者を格納するものである。

【0010】さらに、本発明は、集積回路の内部動作の解析をより困難にするために、プログラマブル論理ゲートの機能を同一に維持したまま、プログラムデータの変更を行うものであり、これらの変更を、集積回路の内部信号、または、集積回路外部からの信号入力を契機として、上記変更を行うものである。

【0011】

【発明の実施の形態および実施例】図 1 は、本発明の第 1 の実施例である集積回路 101 を示す図である。

【0012】集積回路 101 は、プログラマブル論理ゲートを使用して構成された暗号化回路の一例である。このプログラマブル論理ゲートは、4つの論理ブロック $LB1_1$ 、 $LB1_2$ 、 $LB1_3$ 、 $LB1_4$ と複数のスイッチボックス SB とによって構成されている。論理ブロック $LB1_1$ 、 $LB1_2$ 、 $LB1_3$ 、 $LB1_4$ を総称して論理ブロック $LB1$ とした場合、この論理ブロック $LB1$ は、図 1 (2) に示すように、論理ゲート 11 と、 D

10

20

30

40

50

3

FF12と、EEPROM13とによって構成されている。EEPROM13は、暗号化関数を実現するプログラムデータと暗号化鍵データとを格納するものである。

【0013】図1(3)は、上記実施例における暗号化関数の説明図である。集積回路101におけるプログラマブル論理ゲート中に配置されているEEPROM13上に、暗号化回路を特徴づけるプログラムデータdと暗号化鍵データkとが、格納されている。

【0014】また、EEPROM13に格納されているプログラムデータdは、単位論理ブロックLB1₁、LB1₂、LB1₃、LB1₄ 同士の間におけるネットワークを決定するものであり、また、単位論理ブロックLB1₁～LB1₄ のそれぞれが実現する論理関数を決定するものである。

【0015】ところで、図5(1)に示すように、従来の暗号化回路は、汎用のプロセッサによって実現され、平文Pと暗号化鍵データkとを入力し、所定のプログラムを実行することによって、暗号化を行うものである。この場合、汎用プロセッサでは、ハードウェアがモジュール化されているので、このモジュールの入出力端子から信号を取り出すことができ、この取り出された信号を解析することによって、暗号化鍵データを傍受することが可能であり、さらには暗号データの生成の仕組みを傍受することが可能である。観念的には、暗号化関数は、暗号化鍵データkのみによって一意に決まる。

【0016】ところが、上記実施例においては、暗号化関数が、論理ブロックLB1を要素とするプログラマブル論理ゲートによって構成されているので、暗号化関数を特徴づけるパラメータは、暗号化鍵データkとプログラムデータdとの2つになり、従来例におけるパラメータよりも増加する。しかも、これら暗号化鍵データkというパラメータと、プログラムデータdというパラメータとは、ハードウェア上、物理的に1つの不揮発性メモリ(EEPROM13)上に格納されているので、暗号化鍵データkというパラメータとプログラムデータdというパラメータとを、第三者が識別することが困難である。

【0017】すなわち、上記実施例において、暗号文Cは、暗号化鍵データkとプログラムデータdとの両者をパラメータとする関数によって次のように表される。

【0018】 $C = E_k, d(P)$

したがって、暗号化関数を特徴づけるパラメータが、暗号化鍵データkとプログラムデータdの2つになり、暗号化関数のバリエーションが増加する。このために、暗号データ生成のしくみを第三者が解析することは極めて困難である。

【0019】すなわち、上記実施例の暗号化回路構成では、暗号化関数を実現するプログラムデータdと暗号化鍵データkとが、1つのプログラマブル論理ゲート内のメモリに格納され、これらデータd、kを1つのプログ

4

ラムブル論理ゲートの外に出す必要がない。したがって、上記実施例においては、暗号処理を行う場合における意味ある信号が、物理的なモジュールの入出力端子に発生せず、解析の手がかりを第三者に与えにくいという利点がある。

【0020】図2は、本発明の第2の実施例である集積回路102を示す図である。

【0021】集積回路102は、プログラマブル論理ゲートの機能を同一に維持したまま、プログラムデータを変更する実施例であり、論理ブロックLB2₁、LB2₂、LB2₃、LB2₄と、複数のスイッチボックスSBと、プログラムデータ制御ブロックCB1とを有するものである。

【0022】論理ブロックLB2₁は、論理ゲート21と、DFF22と、EEPROM23と、制御部24とを有する。論理ブロックLB2₂、LB2₃、LB2₄のそれぞれの構成は、論理ブロックLB2₁の構成と同様である。

【0023】プログラムデータ制御ブロックCB1は、論理変更手段31と、タイマ32とを有する。論理変更手段31は、プログラマブル論理ゲートの機能を同一に維持したまま、プログラムデータを変更するプログラムデータ変更手段の例であり、タイマ32は、プログラムデータ変更手段(論理変更手段31)を、プログラマブル論理ゲート自身が繰り返して起動する変更起動手段の例である。

【0024】図3は、集積回路102において、プログラマブル論理ゲートの機能を同一に維持したまま、プログラムデータを変更した場合の具体例を示す図である。

【0025】図3(1)に示す集積回路102₁は、集積回路102の具体例であり、論理ブロックLB2₁₁が、ANDゲートとORゲートとによって構成され、論理ブロックLB2₂₁が、ANDゲートとEXNORゲートとによって構成され、論理ブロックLB2₃₁が、NORゲートによって構成され、論理ブロックLB2₄₁が、ANDゲートによって構成されている。

【0026】ここで、プログラムデータを変更することによって、集積回路102₁を、図3(2)に示す集積回路102₂に変更する。つまり、ANDゲートとORゲートとによって構成されている論理ブロックLB2₁₁が、ANDゲートとNORゲートとによって構成されている論理ブロック₁₂に変更され、NORゲートによって構成されている論理ブロックLB2₃₁が、ORゲートによって構成されている論理ブロックLB2₃₂に変更され、論理ブロックLB2₂₁、LB₄₁もそれぞれ論理ブロックLB2₂₂、LB₄₂に変更されている。

【0027】上記変更を実行する場合、プログラムデータ制御ブロックCB1におけるタイマ32が所定時間毎に、トリガ信号を出力し、このトリガ信号に応じて、論理変更手段31が各論理ブロックLB2₁～LB₄に働

きかけ、各論理ブロックLB₂₁～LB₄に設けられているEEPROM23に格納されているプログラムデータdが変化し、これに応じて、論理ゲート21が変化することによって、図3に示すような変更が実行される。

【0028】上記のようにプログラムデータdを変更することによって、図3に示すように、集積回路102₁の論理が集積回路102₂の論理に変更され、しかも、この集積回路102₁の論理を集積回路102₂の論理に変更する場合に、集積回路102₁におけるプログラマブル論理ゲートの機能と集積回路102₂におけるプログラマブル論理ゲートの機能が同一に維持されている。したがって、第三者による集積回路の内部動作の解析がたとえ行われたとしても、その解析が完成されるよりも前に、集積回路の変更が行われるようにタイマ32の周期を設定すれば、第三者による集積回路の内部動作の不正な解析が、現実的には不可能になる。

【0029】上記実施例において、集積回路における論理の変更の契機として、タイマ32の出力信号を使用しているが、この代わりに、カウンタによる所定クロックのカウント完了を、集積回路における論理の変更の契機としてもよい。また、集積回路102に入力される信号が、所定の規格外の信号である場合、この規格外の信号入力を契機として、集積回路における論理の変更を実行するようにしてもよい。このようにすることによって、第三者が内部動作の解析を目的として集積回路102に通常の入力信号とは異なる信号を入力すると、集積回路102における論理の変更が直ちに実行され、集積回路102の内部動作の解析がより困難になる。

【0030】図4は、本発明の第3の実施例である集積回路103を示す図である。

【0031】集積回路103は、プログラマブル論理ゲートの機能を同一に維持したまま、プログラムデータを変更する実施例であり、集積回路103の外部からプログラムデータ変更信号を受け、これによって、プログラマブル論理ゲートの機能を同一に維持したまま、プログラムデータを変更する実施例である。

【0032】また、集積回路103は、論理ブロックLB₂₁、LB₂₂、LB₂₃、LB₂₄と、複数のスイッチボックスSBと、プログラムデータ制御ブロックCB2とを有するものである。プログラムデータ制御ブロックCB2は、集積回路103の外部から受けたプログラムデータ変更信号に基づいて、プログラマブル論理ゲートの機能を同一に維持したまま、プログラムデータを変更する手段である。このようにすれば、プログラマブル論理ゲートの機能を同一に維持したまま、プログラムデータを変更する動作を、集積回路103の外部から、任意に実行させることができる。

【0033】上記実施例において、暗号化関数を実現するプログラムデータを変更する場合、プログラムデータの全部を同時に変更する必要はなく、プログラムデータ

の一部のみを変更するようにしてもよい。

【0034】上記実施例は、暗号化関数を実現する集積回路の一部または全部を、記憶されているプログラムデータの変更によって再構成可能な構造とするものであり、暗号化鍵データと暗号化関数とを実現するプログラムデータの双方を機密情報にしたものである。

【0035】上記実施例によれば、暗号化を特徴づけるプログラムデータと、これらのオペランドとなる暗号化鍵データとを、物理的に同一階層にある記憶回路に分散して格納するので、上記実施例における秘密データと覚しきデータの数が、従来例における秘密データと覚しきデータの数よりも、膨大になり、したがって、不正を働こうとする第三者が解析の起点をつかむことが極めて困難である。

【0036】上記実施例は、暗号化回路についての例であるが、上記実施例において、暗号化回路の代わりに復号化回路を想定し、暗号化鍵データの代わりに復号化鍵データを想定するようにしてもよい。つまり、復号化関数を実現するプログラムデータと復号化鍵データとが、1つのプログラマブル論理ゲート内のメモリに格納されている集積回路を想定してもよい。

【0037】そして、上記復号化においても、プログラマブル論理ゲートの機能を同一に維持したまま、プログラムデータを変更するプログラムデータ変更手段と、上記プログラムデータ変更手段を、プログラマブル論理ゲート自身が繰り返して起動する変更起動手段とを、集積回路が有するようにしてもよい。また、プログラマブル論理ゲートの機能を同一に維持したまま、プログラムデータを変更するとともに、プログラマブル論理ゲートの外部の信号に応じて、プログラムデータの変更動作を起動するプログラムデータ変更手段を、集積回路が有するようにしてもよい。

【0038】この場合、復号化関数を実現する集積回路の一部または全部を、記憶されているプログラムデータの変更によって再構成可能な構造とするものであり、復号化鍵データと復号化関数とを実現するプログラムデータの双方を機密情報にしたものである。また、復号化回路を特徴づけるプログラムデータと、これらのオペランドとなる復号化鍵データとを、物理的に同一階層にある記憶回路に分散して格納するので、上記実施例における秘密データと覚しきデータの数が、従来例における秘密データと覚しきデータの数よりも、膨大になり、したがって、不正を働こうとする第三者が解析の起点をつかむことが極めて困難である。

【0039】さらに、上記実施例において、暗号化回路とともに復号化回路を設けてもよく、この場合、暗号化鍵データとともに復号化鍵データを格納するようにしてもよい。つまり、暗号化関数を実現するプログラムデータと暗号化鍵データと復号化関数を実現するプログラムデータと復号化鍵データとが、1つのプログラマブル論

10

20

30

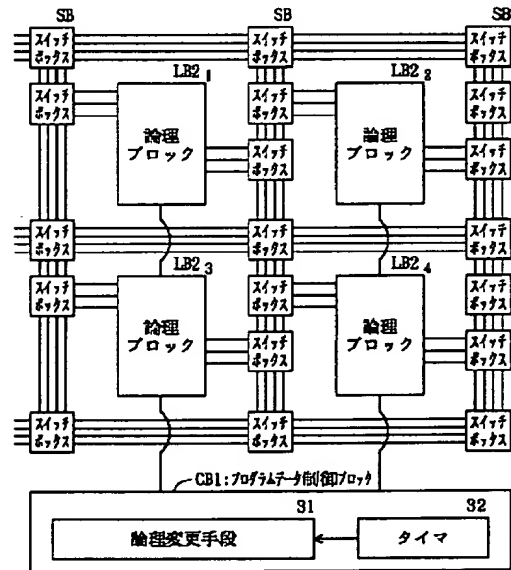
40

50

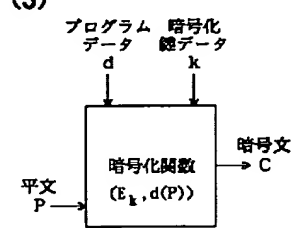
【図3】上記実施例において、同一論理機能を実現しながらプログラムデータを変更した場合の具体例を示す図

【图2】

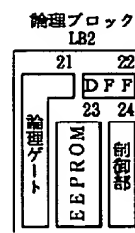
(1) 102: 集積回路



(3)

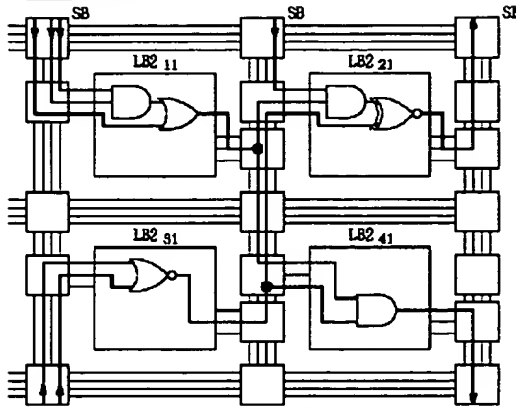
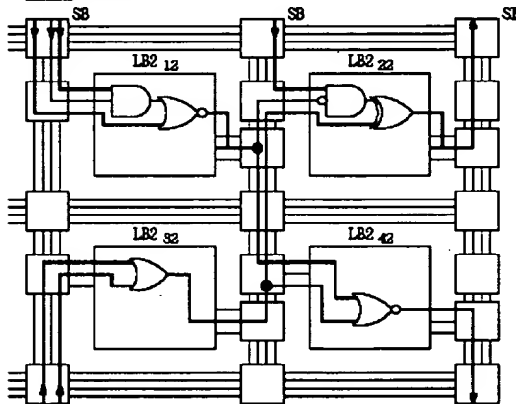


(2)



K4341

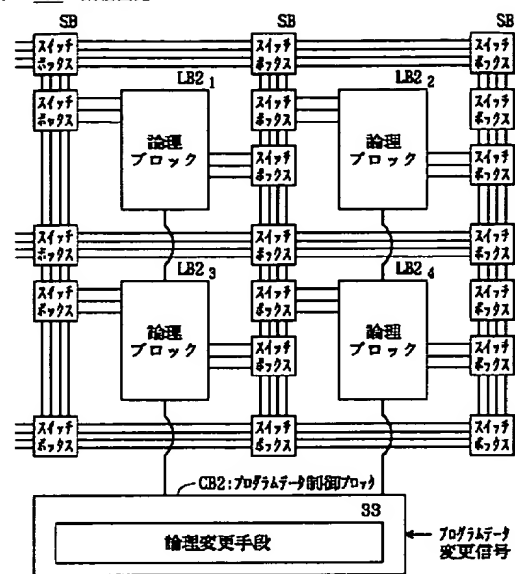
【図3】

(1) 102₁: 集積回路(2) 102₂: 集積回路

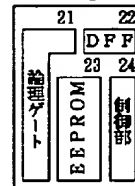
K4341

【図4】

(1) 103: 集積回路



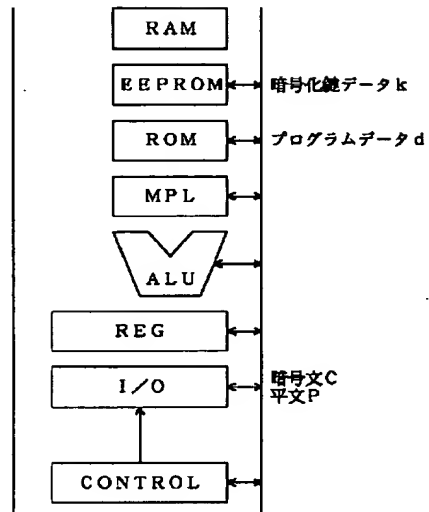
(2) 論理ブロック LB2



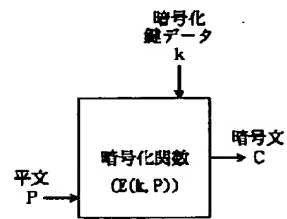
K4341

【図 5】

(1) 100: 従来の集積回路



(2)



K4341